

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

█ S. GRANT AVE.
COLUMBUS, OHIO 43206

Case No. 1:20MJ847

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

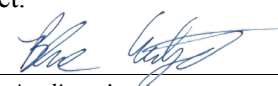
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §§ 1349, 1346 and 1343;	Conspiracy to Commit Honest Services Wire Fraud; and
18 U.S.C. § 1346 and 1343	Honest Services Wire Fraud

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

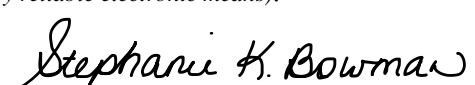

Applicant's Signature

Blane Wetzels, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
FaceTime Video (specify reliable electronic means).

Date: Nov 15, 2020

City and state: Cincinnati, Ohio


Judge's signature

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title



IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:
 [REDACTED] S. GRANT AVE.
 COLUMBUS, OHIO 43206

1:20MJ847

Case No. _____

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, BLANE J. WETZEL, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search [REDACTED] S. Grant Ave., Columbus, Ohio, 43206 (the “PREMISES”) further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (the "FBI"), and have been since August 21, 2016. I am assigned to the Public Corruption Squad of the Cincinnati Division Columbus Resident Agency. In my capacity as a Special Agent, I work on the Southern Ohio Public Corruption Task Force - comprised of various state and federal agencies, and am responsible for investigating violations of federal law, including, but not limited to, public corruption, extortion, bribery, and theft from programs receiving federal funds. I have conducted and participated in public corruption investigations that involved the use of advanced investigative techniques such as the use of: Title III interceptions; confidential human sources; consensually-monitored meetings; execution of search warrants on computers, emails, other electronic communication devices and physical structures; pen register and trap/trace devices; financial

Background on PUCO

² <https://puco.ohio.gov/wps/portal/gov/puco/about-us/resources/mission-and-commitments>

regularly makes decisions that affect the financial outlook of both the energy company and subsidiary.

7. The PUCO is comprised of five commissioners appointed to rotating, five-year terms by the governor of Ohio. “[A]ny Ohioan who is not employed by a public utility and does not have a financial interest in a public utility can apply for an open seat.”³ After considering the resumes of applicants, a 12-person nominating council recommends four finalists to the governor, who either appoints a commissioner from the list or requests another slate of names from the council. The governor’s appointment is confirmed by the Senate.

8. Public Official B is one of five commissioners of PUCO. In fact, Public Official B is the Chairman of PUCO. Public Official B was appointed by the governor of Ohio and designated as Chairman early 2019. Public Official B started his term in office on April 11, 2019. According to PUCO, Public Official B’s term ends on April 10, 2024.⁴

9. Prior to his appointment to the PUCO, Public Official B worked as an attorney for a law firm. Public Official B also had a separate, non-legal consulting arrangement with energy company through an entity called Sustainability Funding Alliance of Ohio Inc., as detailed below. Public Official B retired from his law practice, effective December 31, 2018, prior to his appointment to the PUCO.⁵ The Chairman position occupied by Public Official B, is a full-time position. In his capacity as chairman, Public Official B makes rulings and decisions related to the

³ <https://puco.ohio.gov/wps/portal/gov/puco/about-us/resources/commissioner-appointment-process>

⁴ <https://puco.ohio.gov/wps/portal/gov/puco/about-us/commissioner-bios/chairman-sam-randazzo>

⁵ <https://www.cleveland.com/business/2019/01/governor-dewine-faces-first-major-energy-related-issue-with-puco-commissioner-appointment.html>

The diagram consists of a series of horizontal black bars of different lengths, arranged in a descending staircase pattern from top-left to bottom-right. The bars are arranged in a sequence of 10 rows. The first row has a long bar. The second row has a shorter bar. The third row has a very short bar. The fourth row has a bar of medium length. The fifth row has a bar of medium length. The sixth row has a bar of medium length. The seventh row has a bar of medium length. The eighth row has a bar of medium length. The ninth row has a bar of medium length. The tenth row has a bar of medium length.

[REDACTED]

[REDACTED]

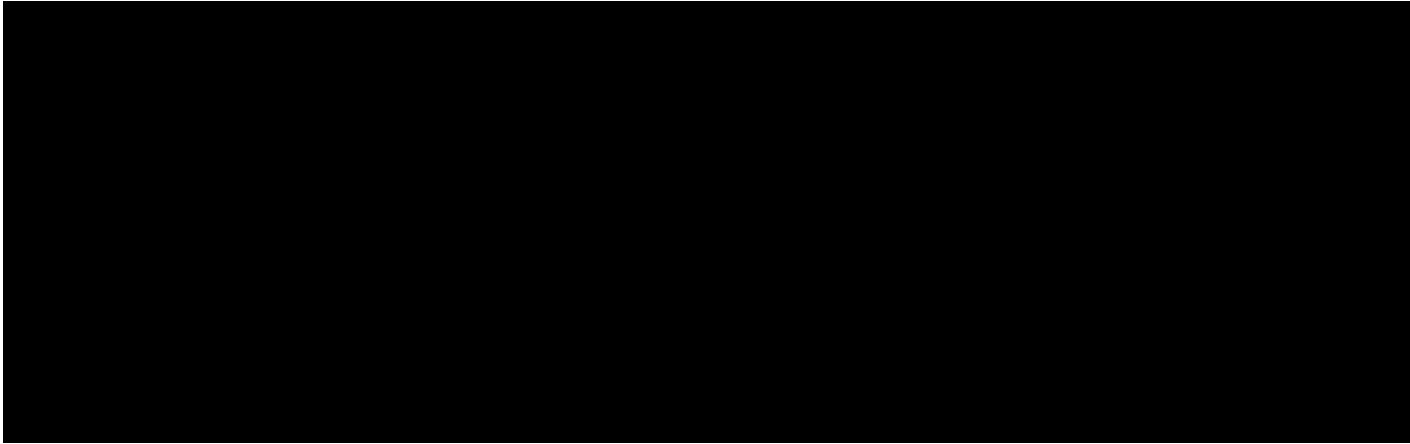
[REDACTED]

[REDACTED]

[REDACTED]

6. [REDACTED]

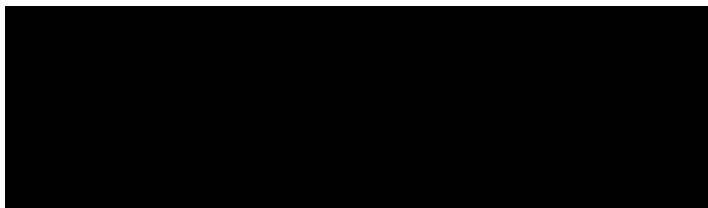
7. [REDACTED]



The PREMISES

38. I have reviewed records from Ohio Bureau of Motor Vehicles, and from that review, I have learned, among other things, that vehicle registration records for Public Official B provide the PREMESIS as his address.

39. I have reviewed records from the energy company, which outline a financial relationship between Public Official B and the energy company. Within the consulting services agreement term sheet, Public Official B's business, SFA, is listed with the PREMESIS as the address of record.



40.



teleworking, makes it even more likely that personal devices like computers will be located at the PREMISES.

44. As referenced above, PUCO employees are currently working from home and therefore it is logical that Public Official B would relocate paper files and other records to his home – the PREMISES. In addition, the PREMISES serves as the address of record for SFA. It is likely that documents, records, and financial instruments related to SFA are contained within the PREMESIS.

45. In my training and experience, electronic evidence, like the evidence recovered during the course of this investigation, can be stored on computers, and may individuals maintain computers in their personal residences. Such electronic evidence can also be stored on cellular phone, and many individuals store cellular phone in their personal residences.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

46. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

48. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where,

and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer

and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

49. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

51. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

52. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

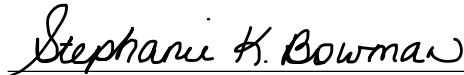
53. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Blane Wetzel
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 15, 2020: **via electronic means, specifically Facetime video.**



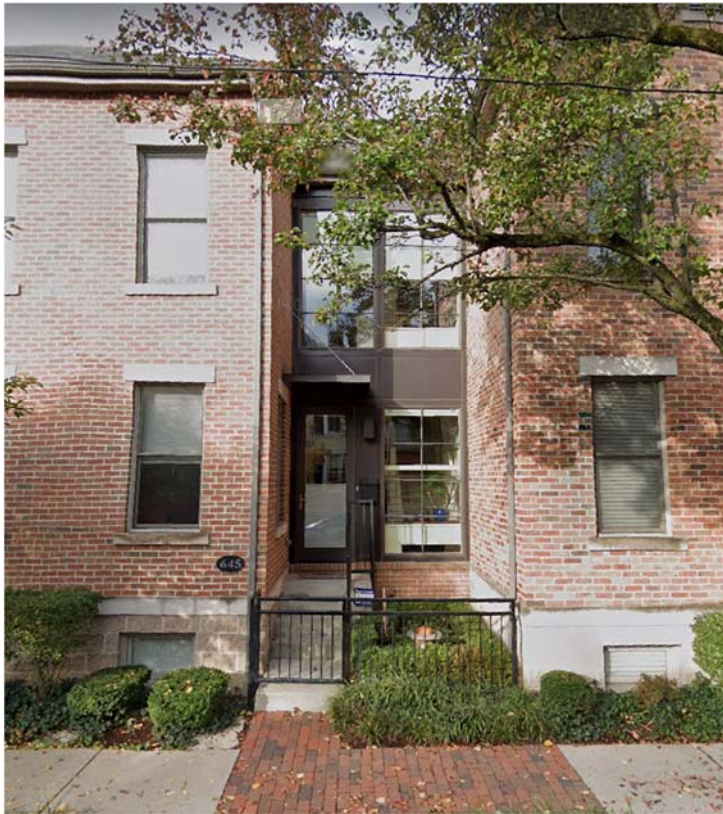
STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to be searched

The property to be searched is [REDACTED] South Grant Avenue, Columbus, Ohio 43206, further described as a two and a half story red brick condominium. The unit is located in the interior section of the eastern side of the complex, which has approximately 19 individual units. Unit [REDACTED] has a clear front door facing Grant Avenue. The number of the unit is shown on a black sign located on the wall south of the door as pictured below.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 1349, 1346, and 1343 those violations involving Samuel Randazzo, Sustainability Funding Alliance of Ohio, Inc., [REDACTED] [REDACTED] and others occurring after September 1, 2018, including:

- a. Records and information relating to honest services wire fraud and a conspiracy to commit honest services wire fraud;
- b. Records and information relating to drafting and passage of legislation to benefit nuclear power plants in Ohio;
- c. Records and information relating to efforts to promote legislative and regulatory policy which favors the energy company, including efforts to enact and implement Ohio HB 6 of 2019, and other regulatory actions before the PUCO, such as information related to resolving contested rate cases and other contested administrative matters, within which the energy company is a stakeholder.
- d. Records and information relating to efforts to nominate and appoint Samuel Randazzo to the Public Utility Commission of Ohio;
- e. Records and information relating the Sustainable Funding Alliance of Ohio, Inc., including financial records, and payments received by and paid by the entity;

- f. Records and information relating to efforts to conceal the criminal activity of Samuel Randazzo, Sustainability Funding Alliance of Ohio, Inc., [REDACTED] [REDACTED] and others;
- g. Records and information relating to the identification of others involved in the conspiracy;
2. Records and information include, but are not limited to, all communications, calendar entries, call lists, voicemails, videos, photographs, images, documents, writings, and notes. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile and cellular phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts, in accordance with filter procedures. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review in accordance with filter procedures.